The Opportunities and Challenges of Change

By the Honorable Michael Wynne
Acting Under Secretary of Defense for Acquisition, Technology and Logistics

Wynne was sworn in as the Deputy Under Secretary of Defense (AT&L) on July 17, 2001. He also served as the Principal Deputy to the Under Secretary of Defense for Acquisition, Technology & Logistics. In 1999, Mr. Wynne retired as Senior Vice President from General Dynamics, where his role was in International Development and Strategy. He spent 23 years with General Dynamics in various senior positions with aircraft (F-16), main battle tanks (M1A2), and space launch vehicles (Atlas and Centaur). He also spent three years with Lockheed Martin, having sold the Space Systems Division to [then] Martin Marietta. He integrated the division into the Astronautics Company and became the general manager of the Space Launch Systems segment, combining the Titan with the Atlas Launch vehicles. Prior to joining industry, Wynne served in the Air Force for seven years, leaving active duty as a captain and assistant professor of astronautics at the U.S. Air Force Academy teaching control theory and fire control techniques. Wynne graduated from the U.S. Military Academy and holds a master's degree in electrical engineering from the Air Force Institute of Technology and a master's degree in business from the University of Colorado.

Acting Under Secretary Wynne's article has been edited from his remarks at AFCEA TechNet International 2004, May 13.

One hundred years ago, the U.S. Army was engaged in a controversial, protracted, irregular war, in a distant land, against insurgent opponents in the Mindanao phase of the Philippine Insurrection. Our military forces were small, composed of volunteers and service professionals. Because of inadequate planning and the stress on forces supporting global expeditionary operations, the military departments began to transform to fight in what we now call Industrial Age warfare.

We got that transformation right — eventually. June 2004 will mark 60 years since the landings in Normandy; arguably the largest joint military operation ever attempted — and we did it while simultaneously executing sizable joint amphibious attacks in the Mariana Islands. We proved supremely adept at fighting Industrial Age warfare. Through its practice we defeated two powerful rivals, secured the safety and prosperity of our own country and those of our allies, and had the means to face down another superpower for over 40 years.

Because the long view in Washington seldom extends past the beginning of an administration, it is tempting to view our current transformation through the lens of the last two years — that is, through our campaigns in Afghanistan and Iraq, each fought with unprecedented, unorthodox methods that highlight not only the superb courage, flexibility and skill of our forces, but the extraordinary technology that we employ in taking the fight to our enemies. Transformation is not unique to our time, it isn't something that happens overnight, and it doesn't happen all by itself. We have to decide, we have to act, and we have to manage our choices.

Current DoD Transformation Efforts

The goal of our current transformation is to enable us to fight war on our terms, which our Director of Transformation, retired Navy Adm. Art Cebrowski, says will mean trading industrial mass for information technology. This is not a matter of simply changing one form of war for another; it's about developing the determination and the capability to change; not once or twice — but as the situation demands. As Art says, "If you are not making any big bets; you are a fixed strategic target and at risk."

One big bet we're making is on network-centric operations. We see this as a path to ensure sustained competitive advantage, and to create new competitive areas — both imperatives if you are serious about creating and sustaining change. On the acquisition side, this means decreasing cycle times and managing the devolution of "sunset" capabilities and processes. It means we're serious about spiral development and about reinvigorating the lost art of system of systems engineering.

Network-centric operations require us to field new kinds of forces. We understand now that the speed of modern warfare creates a continuum, not a succession of phases. Our forces will have to be more expeditionary (lighter, more lethal); capable of precision engagement; able to leverage persistent ISR [intelligence, surveillance and reconnaissance]; with tighter sensor-shooter times, and with expanded unmanned capabilities: Unmanned Aerial Vehicle (UAV); Unmanned Combat Air Vehicle (UCAV); Unmanned Undersea Vehicle (UUV); and robotics.

It's obvious that none of these changes will happen overnight; it's less obvious that we've been struggling with these changes for a generation. At least as far back as the comparatively small, short-legged expedition to Grenada in 1983, we've known where the deficiencies in command and control, battle management and joint operations are. We have exhaustively studied them, then responded with robust management, mind-boggling acronyms, elaborate codification of technical language, long-term commitments to programs and, of course, money. Our command and control bill for the Department continues to grow and is currently at the level of tens of billions of dollars in the POM [Program Objective Memorandum].

During the campaign in Afghanistan, special operations ground controllers needed to tailor the target location data they were sending based on the kind of aircraft that was going to drop the ordnance because different planes take different formats. This is a digital, information age variation of Army and Marine radios that couldn't "net" in Korea or Grenada, or of the incompatible Air Tasking Order formats used by the Air Force and Navy during Operation Desert Storm. The guy on the ground shouldn't have to sort out who it is that is sending help before he can ask for it.

If we're not careful, we're in danger of proliferating the command and control gaps we identified during our transformation to Industrial Age warfare with the speed and efficiency of Information Age systems. While we clearly are in a different era of technology, it is far more important to recognize we are in a different era of national security, with dangerous and immediate threats that demand innovation, practical, near-term responses and efficient resourcing.

Joint Battle Management

I can think of no more critical need than the development and fielding of a joint battle management capability; I see JBMC2 [Joint Interoperability and Integration and Joint Battle Management Command and Control] as not only the path forward, in terms of capability, but also as a test case for system of systems acquisition. A key objective is to provide robust capabilities and innovative approaches for the full spectrum of potential missions using a system of systems approach. This approach to acquisition identifies interdependencies between systems that are related or connected.

We need a "joint plug and play network" that is self-organizing, and built using a mission execution-focused approach. Our future theater C2 structure must ensure that all U.S. and allied forces can act as a unified force. The goal should be to enable the rapid employment of inherently-joint force modules that can operate together en route to and within the theater of war, without extended "shakeout" periods or train-up times. A major initiative we have to improve for the joint warfighter is our JBMC2 Roadmap. The roadmap guides both material and non-material aspects of approximately $47 billion worth of programs within the Department.

The standard for a battle management architecture is deceptively simple, for example: A Navy pilot flying off an aircraft carrier on a strike mission to support a ground force ashore needs to move through and see a common maritime picture while seeing a real-time common air picture. This, among other things, will give updates on the enemy's integrated air defense envelope, then move seamlessly to a common ground picture that will enable a precision strike on precisely the right target ashore — AND — update target effects to determine if a re-attack is necessary.

The Army guy on the ground, who nominated the target, needs to be confident that his sight picture is being sent to that Navy pilot, and that it is being transmitted accurately to the ordnance. And as the guy who called for the strike, he has to know if the results are successful. *Seamlessly — without workarounds, air gaps, data collision or multiple headquarters and command centers managing the mission.*

Think of what we have right now in our information gathering arsenal: JSTARS [Joint Surveillance and Target Attack Radar System] and Rivet Joint; U-2s, Global Hawks, Predators, imagery of every conceivable kind – hyperspectral and infrared; Synthetic Aperture Radar; Humint, Sigint, Masint [Human Intelligence, Signal Intelligence, Measurement and Signatures Intelligence] and; the combat reports of all those dust-covered military personnel reporting over a list of different communications paths as long as my arm.

We understand now that the speed of modern warfare creates a continuum, not a succession of phases.

The questions are:
Will all the information generated by all those systems be available to a unit leader at the platoon or even squad level, to pilots, to logisticians supporting a fast-paced fight or ship captains at sea, providing offshore fires or defeating interdiction threats; and will that information be clear, unambiguous, continuous and reliable?

Other Opportunities

Metrification of the Littorals: The concept of littoral warfare continues to be studied and the expectation for a minimal amount of situational awareness accepted. A key concept within littoral warfare is what I call "metrification" of the littorals, where we would know every square meter, if you will, of a given area or region and have the ability to track all passage through that region. There are a finite number of littoral areas where offensive or defensive operations might occur. Many lie just off the coast of America and some off other continental shelves. This finite list would naturally include the major harbor areas for our shores and some estuaries that the military uses. In the case of our partners, there may be a similar concern and perhaps a larger program envisioned.

The concept of metrification of the littorals would place measuring devices in a lattice work design across this littoral space, making certain that there would be no traffic that could traverse that space without surveillance. The measuring devices would be similar in fashion to the SOSUS [Sound Surveillance System] devices used to good advantage in the Cold War but at an enhanced level of sophistication. This system could be coupled for defensive or offensive operations with other sensors to prepare the battlefield, though it may be covered with water.

At least within our national littorals, this system could be coupled with a form of RFID [Radio Frequency Identification] tagging, with readers being hosted by the buoy system, basically registering both inbound and outbound traffic. When coupled with tagging technology and the current buoy system for channel control, positive control for all the approaches to our coastline could be established. Offensive operations could be

made far easier with this underwater equivalent to C4ISR. In an offensive situation, there might be available differing sensor arrays that could provide confirmation to complete the ISR picture. Thus, the lattice work would provide baseline information for an area, and on-call sensors could provide the rest.

Metrification of High Threat Areas: We have a potential contemporary case study in the six-mile distance between Baghdad International Airport and the city itself. As you know, that stretch of road has proven deadly to our Soldiers. What if we could bring an integrated, networked body of information capabilities to the periodically deadly short stretches. We might be able to parse that one mile down to several increments of several hundred yards. Perhaps we could then parse each of those increments down even further so that we could eventually monitor, anticipate and control each increment efficiently and reliably. But this cannot happen until we press coordinated and integrated signals, combined with fused imagery and human intelligence information to our lowest command levels.

This kind of approach, along with the hard experience of recent military operations, underscores our need to dominate the electromagnetic spectrum — whether it be for protection purposes such as defeating IEDs [Improvised Explosive Devices], or for information warfare purposes to deny enemy situational awareness and disrupt command and control at the same time protecting our own sensors and networks.

The importance of information operations and electronic warfare has been especially apparent in Afghanistan and Iraq. The combined use of kinetic and non-kinetic attacks yielded a pace of operations unmatched by our adversaries. The Department is investing in many promising electronic warfare initiatives to achieve spectrum dominance. We are working to enhance electronic warfare capabilities to provide robust non-kinetic solutions to the warfighter where kinetic effects are undesirable or our rules of engagement dictate non-kinetic actions.

Sense and Respond Logistics: There is a revolution in supply chain management in the private sector: smart tags, real-time links from inventory to production and anticipatory restocking. Our vision for the logistics officer of the future is that he or she will be the commander's combat power manager. At the logistics officer's fingertips will be the precise account of how much combat power (expressed in combat systems, munitions, fuels, replacement stocks) is at hand, and how much will be expended over a given course of action.

This capability is technologically feasible; the Department is looking for a company that can deliver it to us. This is a fertile area, and could use some smart thinking. It is one of the cornerstones of an agile force. Trust in replenishment is as important as trust in indirect fire support.

Challenges

Here's something that keeps me up at night: I fear that each time the Secretary of Defense sees one of those gee-whiz, lightning bolt charts, regardless of whether it's from the Services, the Joint Staff, a unified command or OSD, he really thinks we can do all that stuff. Those charts should force us to think: How many systems do we need? How do we control configuration? Who becomes the central arbiter for canceling the money for redundant systems, and demanding that all the Services and battlefield agencies use common solutions?

Another concern: It's obvious by now that software is the crucial component here, but why is it that software projects are routinely managed so poorly? Where are the systems engineers and the discipline of tools first, product second? Where is it written that software manufacturers do it right the first time and need no discipline and no help? Perhaps it is the culture of speed to market, but we have 13.5 million lines of code for the Future Combat System and 15 million for the Joint Strike Fighter. Frankly, the standard rules of configuration control, requirements flowdown and agreed to content aren't being enforced.

A final, most important concern is changing the culture of power over information. It is no longer enough that flag officers and their staffs have access to the knowledge we can now gather. Information needs to be routinely available, useful and transferable among the squad leaders, helicopter pilots and special operations teams. And it must be accurate, comprehensive, integrated, networked, unambiguous, consistent and reliable. All levels of warfighters must be able to track and engage the enemy remotely. Decision and engagement cycles must be compressed even further. And logistics must complement, not impede, this new pace.

These are fundamentally cultural, not technical, challenges. If we cannot overcome our own cultural barriers, our technical prowess and skill will be wasted. I don't mean to suggest these barriers are malicious obstacles placed deliberately in our path by our predecessors. Face it: Today's tough problems come from yesterday's brilliant solutions. When current culture is no longer useful in solving urgent problems, then we have a professional obligation to change it.

Future electronic warfare systems and sensors should be flexible and enable rapid reprogramming to extend the basic capabilities. They should use common modular components and software to field a common capability on multiple platforms. All of these developments point toward our vision of a lighter footprint, and smaller forces working jointly. The perfect example is trusted fires: A unit in contact calling for help doesn't care what Service or system provides the fire, but it has to trust it will arrive on time, on target.

Whatever networked force we build has to work for both a young infantry captain on the ground and the grizzled ship captain at sea — it has to be accepted, employed and trusted culturally to be effective operationally.

My thoughts have been about change and transformation; there's no let up in the volume or frequency in cries for change. Change is both risk and opportunity. Think differently first, then address change to make it happen. It isn't easy. As Thomas Edison put it, many good opportunities go unnoticed because they show up in overalls and look like work.